Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions

R. Liu, I. Maric, P. Spasojevic, and R.D. Yates

Dept. of ECE, Indian Institute of Science
Bangalore

2nd June 2012

Problem

- To study information-theoretic security for DM interference and broadcast channels
- Secrecy level is measured by the equivocation rate
- Inner and outer bounds on the secrecy capacity regions are derived

Notations

- $\mathbf{X} = [X_1, \ldots, X_n]$
- $A_\epsilon^{(n)}(P_X)$: set of weakly jointly typical sequences $\mathbf{x}$ with respect to $P(x)$

IC with confidential messages

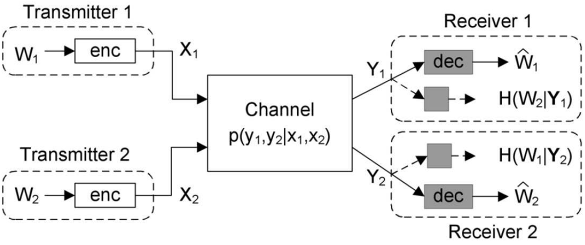


Figure: IC with confidential message

- Channel is memoryless:

  $P(\mathbf{y}_1, \mathbf{y}_2 | \mathbf{x}_1, \mathbf{x}_2) = \prod_{i=1}^{n} P(y_{1i}, y_{2i} | x_{1i}, x_{2i})$
- Stochastic Encoder: Described by a matrix of conditional prob. $f_t(\mathbf{x}_t | w_t)$, where $\mathbf{x}_t \in \mathcal{X}_t^n, w_t \in \mathcal{W}_t$, and

  $\sum f_t(\mathbf{x}_t | w_t) = 1$

- Decoder: $\psi_t : \mathcal{Y}_t \rightarrow \mathcal{W}_t$
- Secrecy level at Rx-t: $\frac{1}{n}H(W_j|\mathbf{Y}_t), t \neq j$
- A rate pair (R_1, R_2) is said to be achievable for the IC with confidential messages if, for any $\epsilon_0 > 0$, there exists a $(M_1, M_2, n, P_e^{(n)})$ code such that
    - $M_t \geq 2^{nR_t}$ for $t = 1, 2$
    - Reliability requirement: $P_e^{(n)} \leq \epsilon_0$
    - Security constraints: $nR_1 - H(W_1|\mathbf{Y}_2) \leq n\epsilon_0$ and $nR_2 - H(W_2|\mathbf{Y}_1) \leq n\epsilon_0$
- Capacity region: closure of the set of all achievable rate pairs (R_1, R_2)

- Let U, V_1 and V_2: auxiliary random variables
- Let π_{IC-I} be the class of distributions that factor as

$$P(u)P(v_1|u)P(v_2|u)P(x_1|v_1)P(x_2|v_2)P(y_1,y_2|x_1,x_2)$$

- Theorem: Let $\mathcal{R}_{IC}(\pi_{IC-I})$ denote the union of all (R_1,R_2) satisfying

$$0 \leq R_1 \leq I(V_1;Y_1|U) - I(V_1;Y_2|V_2,U)$$
$$0 \leq R_2 \leq I(V_2;Y_2|U) - I(V_2;Y_1|V_1,U)$$

over all distributions $P(.)$ in π_{IC-I}. Any rate pair

$$(R_1,R_2) \in \mathcal{R}_{\pi_{IC-I}}$$

is achievable for the IC with confidential messages.

Proof

- An auxiliary random variable U is used in the sense of HK-scheme
- For a given U, two independent stochastic encoders are considered (one for each message)
- Fix $P(u), P(v_1|u)$ and $P(v_2|u)$, and $P(x_1, x_2|v_1, v_2) = P(x_1|v_1)P(x_2|v_2)$ and let

$$R_1^{'} = I(V_1; Y_2|V_2, U) - \epsilon_1$$
$$R_2^{'} = I(V_2; Y_1|V_1, U) - \epsilon_1$$

  where $\epsilon_1(> 0)$ is small for sufficiently large n

Codebook generation

- Randomly generate a typical seq. $\mathbf{u}$ with prob. $P(\mathbf{u}) = \prod_{i=1}^{n} P(u_i)$ and assume that both Tx and Rx know $\mathbf{u}$
- For Tx-t, generate $2^{n(R_t+R_t^{'})}$ independent seq. $\mathbf{v_t}$ each with prob. $P(\mathbf{v}_t|\mathbf{u})$ and labeled as

$$\mathbf{v}_t(w_t, k_t), w_t \in \{1, \ldots, M_t\}, k_t \in \{1, \ldots, M_t^{'}\}$$

  where $M_t = 2^{nR_t}$ and $M_t^{'} = 2^{nR_t^{'}}$
- Let $\mathcal{C}_t = \{\mathbf{v}_t(w_t, k_t),\ \text{for all } (w_t, k_t)\}$: codebook of Tx-t
- Its w_tth bin or subcodebook

$$\mathcal{C}_t(w_t) = \{\mathbf{v}_t(w_t, k_t),\ \text{for } k_t = 1, \ldots, M_t^{'}\}$$

Encoding

- To send a message pair $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, each Tx employs a stochastic encoder
- Encoder t randomly chooses an element $\mathbf{v}_t(w_t, k_t)$ from the subcodebook $\mathcal{C}_t(w_t)$
- Tx generates the channel input seq. based on mappings $P(x_i|v_i)$

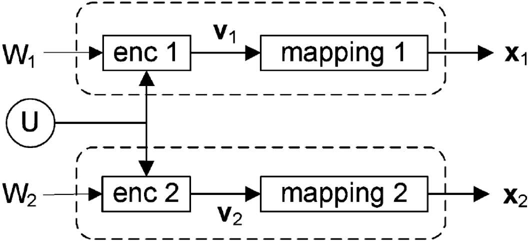


Figure: Code construction for IC-CM

Decoding

- Given a typical seq. $\mathbf{u}$, let $A_{\epsilon}^{(n)}(P_{V_t,Y_t|U})$ denote the set of jointly typical seq. $\mathbf{v_t}$ and $\mathbf{y}_t$ with respect to $P(v_t, y_t|u)$
- Decoder t chooses w_t so that

$$(\mathbf{v_t}(w_t, k_t), \mathbf{y}_t) \in A_{\epsilon}^{(n)}(P_{V_t,Y_t|U})$$

when such w_t exists and is unique; otherwise, an error is declared

Error probability analysis

- Define the following events

$$E_t(w_t, k_t) = \{(\mathbf{v}_t(w_t, k_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(P_{V_t, Y_t|U})\}$$
$$K_1 = \{\mathbf{v}_1(1,1) \text{ sent}\}$$

- Union bound on the error probability of receiver 1

$$\begin{aligned} P_{e,1}^{(n)} &\leq P\left\{\bigcap_{k_1} E_1^c(1, k_1)|K_1\right\} + \sum_{w_1 \neq 1, k_1} P\{E_1(w_1, k_1)|K_1\} \\ &\leq P\{E_1^c(1,1)|K_1\} + \sum_{w_1 \neq 1, k_1} P\{E_1(w_1, k_1)|K_1\} \qquad (1) \end{aligned}$$

- From joint AEP:

$$P\{E_1^c(1,1)|K_1\} \le \epsilon \tag{2}$$

and

$$P\{E_1(w_1,k_1)|K_1\} \le 2^{-n[I(V_1;Y_1|U)-\epsilon]} \tag{3}$$

- If $R_1 + R_1' < I(V_1;Y_1|U)$, then $P_{e,1}^{(n)} \le \epsilon_0$ for sufficiently large n.

Equivocation calculation

- Need to show following:

$$nR_1 - H(W_1|\mathbf{Y}_2) \leq n\epsilon_0$$

- $H(W_1|\mathbf{Y}_2) \geq H(W_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U})$

$$
\begin{aligned}
& H(W_1|\mathbf{Y}_2) \\
& \geq H(W_1, \mathbf{V}_1|\mathbf{V}_2, \mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) \\
& \qquad -H(\mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) + H(\mathbf{Y}_2|\mathbf{V}_1, \mathbf{V}_2, \mathbf{U}) \\
& \geq H(\mathbf{V}_1|\mathbf{V}_2, \mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) - I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) \quad (4)
\end{aligned}
$$

- Consider the first term in (4)

$$
\begin{aligned}
H(\mathbf{V}_1|\mathbf{V}_2, \mathbf{U}) &= H(\mathbf{V}_1|\mathbf{U}) \\
&= \log M_1 M_1' = n(R_1 + R_1') \qquad (5)
\end{aligned}
$$

- Using joint-typical argument, it can be shown that

$$
H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) \leq n\epsilon_2 \qquad (6)
$$

- It can also be shown that

$$I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \leq nI(V_1;Y_2|V_2,U) + n\epsilon_3 \tag{7}$$

- From (5) - (7), (4) becomes:

$$\begin{aligned} H(W_1|\mathbf{Y}_2) &\geq n(R_1 + R_1^{'}) - n\epsilon_2 - nI(V_1;Y_2|V_2,U) - n\epsilon_3 \\ &= nR_1 - n\epsilon_4, \qquad \text{where, } \epsilon_4 = \epsilon_1 + \epsilon_2 + \epsilon_3 \end{aligned} \tag{8}$$

Outer bound for IC-CM

Theorem

Let $\mathcal{R}_O(\pi_{IC-O})$ denote the union of all (R_1, R_2) satisfying

$$
\begin{aligned}
R_1 \leq \min\{& I(V_1; Y_1|U) - I(V_1; Y_2|U), \\
& I(V_1; Y_1|V_2, U) - I(V_1; Y_2|V_2, U)\} \qquad (9) \\
R_2 \leq \min\{& I(V_2; Y_2|U) - I(V_2; Y_1|U), \\
& I(V_2; Y_2|V_1, U) - I(V_2; Y_1|V_1, U)\} \qquad (10)
\end{aligned}
$$

over all distributions $P(.)$ in π_{IC-O}. For the IC $(\mathcal{X}_1 \times \mathcal{X}_2, P(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with confidential messages, the capacity region

$$\mathcal{C}_{IC} \subseteq \mathcal{R}_O(\pi_{IC-O})$$

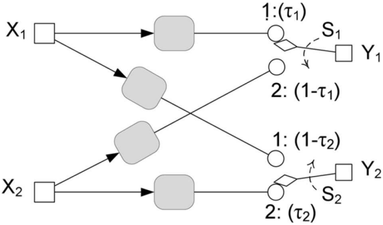
π_{IC-O} is the class of distributions that factor as:

$$P(u)P(v_1, v_2|u)P(x_1|v_1)P(x_2|v_2)P(y_1, y_2|x_1, x_2)$$

Outer bound for IC-CM

- First outer bound
  - Reliable transmission requirement
  - Security constraint
- Second outer bound
  - Genie gives Rx-1 message W_2
  - Rx-2 evaluates the equivocation with W_2 as side information

Switch channel (SC)



- SC can not listen to both transmissions at the same time
- Each Rx has a random switch $s_t \in \{1, 2\}$

$$P(S_{t,i} = t) = \tau_t, \text{ and } P(S_{t,i} = \bar{t}) = 1 - \tau_t, \quad i = 1, \ldots, n$$

Switch channel

Theorem

For the switch channel with confidential messages, the capacity region $\mathcal{C}_{SC}$ is the union of all (R_1, R_2) satisfying

$$R_1 \leq I(V_1; Y_1|U) - I(V_1; Y_2|V_2, U)$$
$$R_2 \leq I(V_2; Y_2|U) - I(V_2; Y_1|V_1, U)$$

over all distributions $P(.)$ in π_{IC-I}

- When $\tau_1 = \tau_2 = 1$, SC-CM reduces to two independent parallel channels without the secrecy constraints
- When $\tau_1 = 1$ and $\tau_2 = 0$, SC-CM reduces to wiretap channel

Broadcast channel

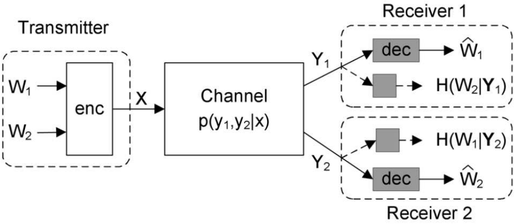


Figure: BC with confidential messages

Inner bound

- Consider the class of distributions $P(u, v_1, v_2, x, y_1, y_2)$ (denoted as (π_{BC})) that factor as

$$P(u)P(v_1, v_2|u)P(x|v_1, v_2)P(y_1, y_2|x)$$

- *Theorem:* Let $\mathcal{R}_{BC}(\pi_{BC})$ denote the union of all (R_1, R_2) satisfying

$$\begin{aligned} & R_1, R_2 \geq 0 \\ & R_1 \leq I(V_1; Y_1|U) - I(V_1; V_2|U) - I(V_1; Y_2|V_2, U) \\ & R_2 \leq I(V_2; Y_2|U) - I(V_1; V_2|U) - I(V_2; Y_1|V_1, U) \end{aligned}$$

over all distributions $P(.)$ in π_{BC}. Any rate pair

$$(R_1, R_2) \in \mathcal{R}_{BC}(\pi_{BC})$$

is achievable for the BC with confidential messages.

Proof

- Based on: double-binning scheme which combines Gel'fand-Pinsker binning and the random binning
- A joint encoder is used to generate two codewords $\mathbf{v}_1$ and $\mathbf{v}_2$, one for each messages W_1 and W_2
- Fix $P(u), P(v_1|u)$, $P(v_2|u)$ and $P(x|v_1, v_2)$ and define

$$R_1^{'} = I(V_1; Y_2|V_2, U) - \epsilon_1^{'}$$
$$R_2^{'} = I(V_2; Y_1|V_1, U) - \epsilon_1^{'}$$
$$R^{\dagger} = I(V_1; V_2|U) + \epsilon_1^{'}$$

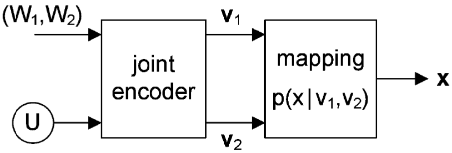


Figure: Code construction for BC-CM

Codebook generation

- Generate randomly a typical sequence **u** with probability $P(\mathbf{u}) = \prod_{i=1}^{n} P(u_i)$ and assume that both the Tx and Rx know the seq. **u**

- Generate $2^{R_t + R_t' + R^\dagger}$ independent seq. $\mathbf{v}_t$ each with prob. $P(\mathbf{v}_t|\mathbf{u})$ and label them

$$\mathbf{v}_t(w_t, s_t, k_t), \;\; w_t \in \{1, \ldots, M_t\}, s_t \in \{1, \ldots, J_t\} \text{ and } k_t \in \{1, \ldots, G_t\}$$

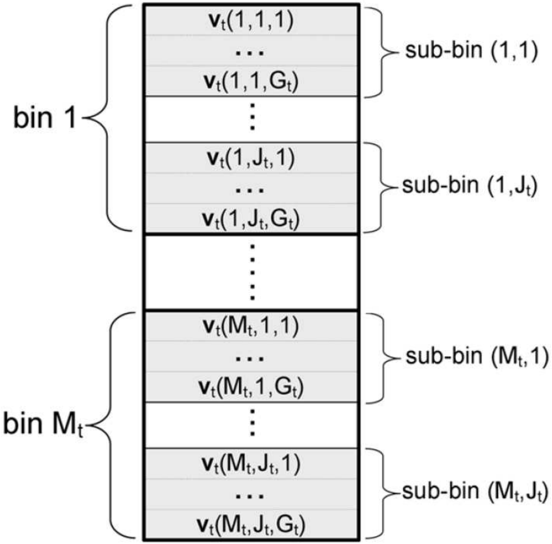
where $M_t = 2^{nR_t}, J_t = 2^{nR_t'}$ and $G_t = 2^{nR^\dagger}$

- $\mathcal{C}_t = \{\mathbf{v}_t(w_t, s_t, k_t),\ \text{for all } (w_t, s_t, k_t)\}$: Tx-t codebook
- The codebook $\mathcal{C}_t$ is partitioned into M_t bins, and the w_tth bin is

$$\mathcal{C}_t(w_t) = \{\mathbf{v}_t(w_t, s_t, k_t),\ \text{for } s_t \in \{1, \ldots, J_t\}. \\ k_t \in \{1, \ldots, G_t\}\}$$

- Each bin $\mathcal{C}_t(w_t)$ is divided into J_t sub-bins and the (w_t, s_t)th sub-bin is:

$$\mathcal{C}_t(w_t, s_t) = \{\mathbf{v}_t(w_t, s_t, k_t),\ \text{for } k_t \in \{1, \ldots, G_t\}\}$$



$\mathbf{v}_t(1,1,1)$
...
$\mathbf{v}_t(1,1,G_t)$
sub-bin (1,1)
bin 1
$\mathbf{v}_t(1,J_t,1)$
...
$\mathbf{v}_t(1,J_t,G_t)$
sub-bin $(1,J_t)$
$\mathbf{v}_t(M_t,1,1)$
...
$\mathbf{v}_t(M_t,1,G_t)$
sub-bin $(M_t,1)$
bin M_t
$\mathbf{v}_t(M_t,J_t,1)$
...
$\mathbf{v}_t(M_t,J_t,G_t)$
sub-bin (M_t,J_t)

Encoding

- To send message pair $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, the Tx employs a stochastic encoder
- Randomly choose a sub-bin $\mathcal{C}_t(w_t, s_t)$ from the bin $\mathcal{C}_t(w_t)$, for $t = 1, 2$
- Select a pair (k_1, k_2) so that

$$(\mathbf{v}_1(w_1, s_1, k_1), (\mathbf{v}_2(w_2, s_2, k_2)) \in A_\epsilon^{(n)}(P_{V_1, V_2|U})$$

where $A_\epsilon^{(n)}(P_{V_1, V_2|U})$: set of jointly typical seq. $\mathbf{v}_1$ and $\mathbf{v}_2$ with respect to $P(v_1, v_2|u)$ given $\mathbf{u}$

- Generate the channel input seq. according to $P(x|v_1, v_2)$

Decoding

- Decoder t chooses w_t so that

$$(\mathbf{v}_t(w_t, s_t, k_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(P_{V_t, Y_t|U})$$

  where $A_\epsilon^{(n)}(P_{V_t, Y_t|U})$: set of jointly typical seq. $\mathbf{v}_t$ and $\mathbf{y}_t$ with respect to $P(v_t, y_t|u)$ for a given typical seq. $\mathbf{u}$
- If w_t is not unique or no such w_t exists, then an error is declared

- Decoding and encoding error
- Equivocation calculation is similar to IC-CM
- Outer bound expression is same but difference in the input distribution over which it is optimized